

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-122238

(43)Date of publication of application : 30.04.1999

(51)Int.Cl. H04L 9/08
 G06K 17/00
 G09C 1/00
 H04L 9/14
 H04L 9/32

(21)Application number : 09-284785

(71)Applicant : RICOH CO LTD

(22)Date of filing : 17.10.1997

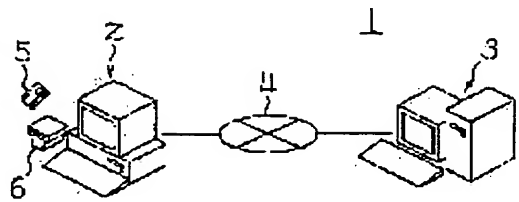
(72)Inventor : KANAI YOICHI

(54) NETWORK SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a network system capable of updating an authentication key independently of whether the communication algorithm is a symmetry key cipher system or an asymmetry key cipher system.

SOLUTION: After mutual authentication conducted by using an (m-1)th internal authentication key and an (n-1)th external authentication key is established, a server 3 sends random numbers Rk1, Rk2 to a client 2, the random numbers Rk1, Rk2 are encrypted by using the (m-1)th internal authentication key and the (n-1)th external authentication key used for the mutual authentication to generate newly the m-th internal authentication key and the n-th external authentication key and they are stored in a nonvolatile memory.



LEGAL STATUS

[Date of request for examination]

17.02.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-122238

(43) 公開日 平成11年(1999) 4月30日

(51) Int.Cl. ⁸	識別記号	F I	
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 D
G 0 6 K 17/00		G 0 6 K 17/00	T
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 E
H 0 4 L 9/14		H 0 4 L 9/00	6 0 1 E
9/32			6 4 1
審査請求 未請求 請求項の数11 O L (全 16 頁) 最終頁に続く			

(21) 出願番号 特願平9-284785

(22) 出願日 平成9年(1997)10月17日

(71) 出願人 000006747

株式会社リコー

東京都大田区中馬込1丁目3番6号

(72) 発明者 金井 洋一

東京都大田区中馬込1丁目3番6号 株式会社リコー内

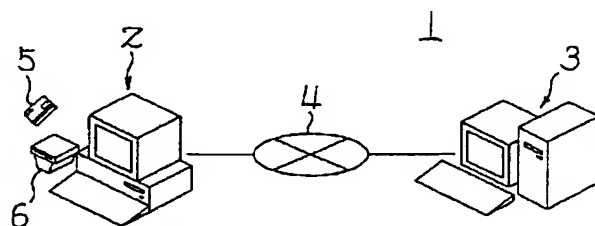
(74) 代理人 弁理士 柏木 明 (外1名)

(54) 【発明の名称】 ネットワークシステム

(57) 【要約】

【課題】 通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、認証鍵を更新することができるネットワークシステムを提供する。

【解決手段】 (m-1) 番の内部認証鍵と、(n-1) 番の外部認証鍵を用いて行なう相互認証が成立した後に、サーバ3から乱数Rk1、Rk2をクライアント2に送信し、前記相互認証に用いた(m-1) 番の内部認証鍵と、(n-1) 番の外部認証鍵を用いて乱数Rk1、Rk2を暗号化して、m番の内部認証鍵とn番の外部認証鍵を新たに生成して、不揮発性メモリに記憶する。



【特許請求の範囲】

【請求項 1】 通信回線を介して接続されているクライアントとサーバとの間の相互認証に使用する認証鍵を格納している記憶媒体をユーザが所持し、この記憶媒体と前記クライアントを接続して、前記認証鍵を用いた前記相互認証を行なった後、前記認証鍵に基づいてセッション鍵を生成して暗号化通信を行なうネットワークシステムであって、

前記認証鍵は前記記憶媒体に複数個記憶して、定期または不定期に更新して用い、

この更新を前記複数の認証鍵のうちいずれかのものに対して行なうには、少なくとも当該認証鍵以外の前記認証鍵を用いて行なう前記相互認証が成立した後に、前記サーバから乱数を前記クライアントに送信し、前記相互認証に用いた前記認証鍵を用いて前記乱数から更新にかかる前記認証鍵を新たに生成して前記記憶媒体に記憶することにより行なうものであることを特徴とするネットワークシステム。

【請求項 2】 記憶媒体は、クライアントがサーバを認証するための認証鍵である外部認証鍵と、前記サーバが前記クライアントを認証するための認証鍵である内部認証鍵とをいずれも識別番号を付して複数個ずつ記憶していて、前記内部認証鍵および前記外部認証鍵を用いて相互認証を行なうものであることを特徴とする請求項 1 に記載のネットワークシステム。

【請求項 3】 複数の内部認証鍵のうち識別番号が m 番のものを更新するには、外部認証鍵と少なくともこの m 番の内部認証鍵以外の内部認証鍵とを用いて行なう相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記 m 番の内部認証鍵を新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とする請求項 2 に記載のネットワークシステム。

【請求項 4】 複数の外部認証鍵のうち識別番号が n 番のものを更新するには、内部認証鍵と少なくともこの n 番の外部認証鍵以外の外部認証鍵とを用いて行なう相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記 n 番の外部認証鍵を新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とする請求項 1 または 2 に記載のネットワークシステム。

【請求項 5】 複数の内部認証鍵のうち識別番号が m 番のものおよび複数の外部認証鍵のうち識別番号が n 番目のものを一度に更新するには、少なくとも前記 m 番の内部認証鍵以外の内部認証鍵と少なくとも前記 n 番の外部認証鍵以外の外部認証鍵とを用いて行なう相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を

用いて前記乱数から前記 m 番の内部認証鍵と前記 n 番の外部認証鍵とを新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とする請求項 2、

3、4 のいずれかに記載のネットワークシステム。

【請求項 6】 複数の内部認証鍵を一度に更新するには、外部認証鍵と識別番号が m 番より小さい内部認証鍵とを用いて相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記識別番号が m 番以上の各内部認証鍵を新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とする請求項 2、3、4、5 のいずれかに記載のネットワークシステム。

【請求項 7】 複数の外部認証鍵を一度に更新するには、内部認証鍵と識別番号が n 番より小さい外部認証鍵とを用いて相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記識別番号が n 番以上の各外部認証鍵を新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とする請求項 2、3、4、5、6 のいずれかに記載のネットワークシステム。

【請求項 8】 複数の内部認証鍵と複数の外部認証鍵とを一度に更新するには、識別番号が m 番より小さい内部認証鍵と識別番号が n 番より小さい外部認証鍵とを用いて行なう相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から識別番号が m 番以上の内部認証鍵と識別番号が n 番移動の外部認証鍵とを新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とする請求項 2、3、4、5、6、7 のいずれかに記載のネットワークシステム。

【請求項 9】 更新の際の内部認証鍵の総数を M 、外部認証鍵の総数を N としたときに、下式で示される m 番目の内部認証鍵と n 番目の外部認証鍵の更新は、識別番号が少なくとも n 番より小さい番号の外部認証鍵を用いてクライアントがサーバを認証したことを条件に行なうものであることを特徴とする請求項 2、3、4、5、6、7、8 のいずれかに記載のネットワークシステム。

$$M - m = N - n$$

【請求項 10】 記憶媒体は、更新に先立って行なわれた相互認証に使用した認証鍵を用いサーバがクライアントに送信した乱数から新たな認証鍵の生成を行なって、この生成後の新たな認証鍵を記憶媒体内部の不揮発性メモリにのみ記憶するものであることを特徴とする請求項 1、2、3、4、5、6、7、8、9 のいずれかに記載のネットワークシステム。

【請求項 11】 記憶媒体として IC カードを用いることを特徴とする請求項 1、2、3、4、5、6、7、8、9、10 のいずれかに記載のネットワークシステム。

ム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明はネットワークシステムに関し、特に、クライアントとサーバとの間の相互認証に関する。

【0002】

【従来の技術】特開平6-150082号公報には、ICカードを所持したユーザが、このICカードに記録されている秘密情報を用い、通信回線を介しクライアントからサーバに対して認証を要求する技術に関するものであり、非対称鍵暗号方式の暗号アルゴリズムを用いてICカード内の秘密情報を変更する技術が開示されている。

【0003】

【発明が解決しようとする課題】しかしながら、前記従来技術は、秘密鍵と公開鍵を用いる非対称鍵暗号方式の暗号アルゴリズムをICカードに搭載してICカード内の秘密情報を変更する技術が開示されているにとどまり、対称鍵暗号方式を用いる場合にICカード内の秘密情報を変更するための技術はなんら開示されていない。

【0004】この発明の目的は、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、認証鍵を更新することができるネットワークシステムを提供することにある。

【0005】この発明の別の目的は、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、内部認証鍵や外部認証鍵を更新することができるネットワークシステムを提供することにある。

【0006】この発明の別の目的は、少ない鍵更新処理により安全に、内部認証鍵や外部認証鍵を更新することができるネットワークシステムを提供することにある。

【0007】この発明の別の目的は、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、使用が稀である認証鍵により使用が頻繁な内部認証鍵や外部認証鍵を安全に更新することができるネットワークシステムを提供することにある。

【0008】この発明の別の目的は、更新後の新たな認証鍵を記憶媒体外に漏らすことなく認証鍵を安全に更新することができるネットワークシステムを提供することにある。

【0009】この発明の別の目的は、ネットワークシステムを低コストで構築することにある。

【0010】

【課題を解決するための手段】請求項1に記載の発明は、通信回線を介して接続されているクライアントとサーバとの間の相互認証に使用する認証鍵を格納している記憶媒体をユーザが所持し、この記憶媒体と前記クライアントを接続して、前記認証鍵を用いた前記相互認証を行なった後、前記認証鍵に基づいてセッション鍵を生成

して暗号化通信を行なうネットワークシステムであって、前記認証鍵は前記記憶媒体に複数個記憶して、定期または不定期に更新して用い、この更新を前記複数の認証鍵のうちいずれかのものに対して行なうには、少なくとも当該認証鍵以外の前記認証鍵を用いて行なう前記相互認証が成立した後に、前記サーバから乱数を前記クライアントに送信し、前記相互認証に用いた前記認証鍵を用いて前記乱数から更新にかかる前記認証鍵を新たに生成して前記記憶媒体に記憶することにより行なうものであることを特徴とするものである。

【0011】従って、相互認証が成立した後に、サーバから乱数をクライアントに送信し、相互認証に用いた認証鍵を用いて乱数から更新にかかる認証鍵を新たに暗号化や復号化などで生成することができるので、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、認証鍵を更新することができる。

【0012】請求項2に記載の発明は、記憶媒体は、クライアントがサーバを認証するための認証鍵である外部認証鍵と、前記サーバが前記クライアントを認証するための認証鍵である内部認証鍵とをいずれも識別番号を付して複数個ずつ記憶していて、前記内部認証鍵および前記外部認証鍵を用いて相互認証を行なうものであることを特徴とするものである。

【0013】従って、相互認証が成立した後に、サーバから乱数をクライアントに送信し、相互認証に用いた内部認証鍵を用いて乱数から更新にかかる内部認証鍵、外部認証鍵を新たに生成することができるので、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、内部認証鍵、外部認証鍵を更新することができる。

【0014】請求項3に記載の発明は、複数の内部認証鍵のうち識別番号がm番のものを更新するには、外部認証鍵と少なくともこのm番の内部認証鍵以外の内部認証鍵とを用いて行なう相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記m番の内部認証鍵を新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とするものである。

【0015】従って、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、識別番号がm番の内部認証鍵を更新することができる。

【0016】請求項4に記載の発明は、複数の外部認証鍵のうち識別番号がn番のものを更新するには、内部認証鍵と少なくともこのn番の外部認証鍵以外の外部認証鍵とを用いて行なう相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記n番の外部認証鍵を新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とするものである。

ある。

【0017】従って、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに識別番号が n 番の外部認証鍵を更新することができる。

【0018】請求項5に記載の発明は、複数の内部認証鍵のうち識別番号が m 番のものおよび複数の外部認証鍵のうち識別番号が n 番目のものを一度に更新するには、少なくとも前記 m 番の内部認証鍵以外の内部認証鍵と少なくとも前記 n 番の外部認証鍵以外の外部認証鍵とを用いて行なう相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記 m 番の内部認証鍵と前記 n 番の外部認証鍵とを新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とするものである。

【0019】従って、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、少ない鍵更新処理により安全に、識別番号が m 番の内部認証鍵と識別番号が n 番の外部認証鍵を一度に更新することができる。

【0020】請求項6に記載の発明は、複数の内部認証鍵を一度に更新するには、外部認証鍵と識別番号が m 番より小さい内部認証鍵とを用いて相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記識別番号が m 番以上の各内部認証鍵を新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とするものである。

【0021】従って、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、少ない鍵更新処理により安全に、複数の内部認証鍵を一度に更新することができる。

【0022】請求項7に記載の発明は、複数の外部認証鍵を一度に更新するには、内部認証鍵と識別番号が n 番より小さい外部認証鍵とを用いて相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記識別番号が n 番以上の各外部認証鍵を新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とするものである。

【0023】従って、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、少ない鍵更新処理により安全に、複数の外部認証鍵を一度に更新することができる。

【0024】請求項8に記載の発明は、複数の内部認証鍵と複数の外部認証鍵とを一度に更新するには、識別番号が m 番より小さい内部認証鍵と識別番号が n 番より小さい外部認証鍵とを用いて行なう相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前

記乱数から識別番号が m 番以上の内部認証鍵と識別番号が n 番移動の外部認証鍵とを新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とするものである。

【0025】従って、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、少ない鍵更新処理により安全に、複数の内部認証鍵と複数の外部認証鍵とを一度に更新することができる。

【0026】請求項9に記載の発明は、更新の際の内部認証鍵の総数を M 、外部認証鍵の総数を N としたときに、下式で示される m 番目の内部認証鍵と n 番目の外部認証鍵の更新は、識別番号が少なくとも n 番より小さい番号の外部認証鍵を用いてクライアントがサーバを認証したことを条件に行なうものであることを特徴とするものである。

$$【0027】M-m=N-n$$

従って、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、使用が稀である認証鍵により使用が頻繁な認証鍵 m 番目の内部認証鍵と n 番目の外部認証鍵とを安全に更新することができる。

【0028】請求項10に記載の発明は、記憶媒体は、更新に先立って行なわれた相互認証に使用した認証鍵を用いサーバがクライアントに送信した乱数から新たな認証鍵の生成を行なって、この生成後の新たな認証鍵を記憶媒体内部の不揮発性メモリにのみ記憶するものであることを特徴とするものである。

【0029】従って、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、更新後の新たな認証鍵を記憶媒体外に漏らすことなく認証鍵を安全に更新することができる。

【0030】請求項11に記載の発明は、記憶媒体としてICカードを用いることを特徴とするものである。

【0031】従って、一般に普及し始めているICカードを記憶媒体として用い、ネットワークシステムを低コストで構築することができる。

【0032】

【発明の実施の形態】

【発明の第1の実施の形態】図1は、この発明のネットワークシステムを実現した、この発明の第1の実施の形態である対称鍵暗号系を使用したネットワークシステム1の概略システム構成のブロック図である。

【0033】ネットワークシステム1は、クライアント2と、このクライアントを管理するクライアント管理データベース（図示せず）を備えたサーバ3とを通信回線4で接続したクライアント／サーバシステムである。

【0034】クライアント2には、ICカード5に対してデータの書き込み、読み取りを行なうICカードリーダー6が接続されている。

【0035】サーバ3は、ICカード5の配布元や、後述する秘密鍵の発行センタをも兼ねている。すなわち、

サーバ3は、各ユーザに対応して、ユーザ用に秘密鍵をm組生成し、また、サーバ3用に秘密鍵をn組生成する（このサーバ3用に秘密鍵は、各ユーザごとに生成せず、全ユーザ共通としてもよい）。そして、サーバ3のクライアント管理データベースには、サーバ3が生成したすべての秘密鍵を記憶する。

【0036】ICカード5は、この発明の記憶媒体を実現するもので、例えば、図2に示すように、マイクロプロセッサ11と、このマイクロプロセッサ11と接続され、データの書換えが可能な不揮発性メモリ12（EEPROM〔この発明の記憶手段を実現するものである〕）と、マイクロプロセッサ11とICカードリーダー6との間のデータの授受を行なうインターフェイスである入出力装置13などが搭載されていて、国際規格（IS）で規定されている、“Internal Authentication コマンド”、“External Authentication コマンド”、“Get Challenge コマンド”をサポートしているものである。

【0037】マイクロプロセッサ11のROMには、クライアント2とサーバ3との間の相互認証を行なう暗号アルゴリズムが記憶されている。この暗号アルゴリズムはサーバ3（のROM）にも格納されている。このマイクロプロセッサ11およびサーバ3のROMに記憶されている相互認証のための暗号アルゴリズムは非対称鍵暗号方式のものである。

【0038】図3は、不揮発性メモリ12内の認証鍵のファイルフォーマットの一例を示すブロック図である。このファイルフォーマットは、主ファイルMFの下位に専用ファイルDFを有し（図3の例では、専用ファイルDF1、DF2、DF3を有している）、この専用ファイルDFの下位に基礎ファイルIEFを有する（図3の例では、専用ファイルDF1の下位に基礎ファイルIEF1、IEF2、IEF3、IEF4、IEF5、IEF6、IEF7を有している）階層構造をなしている。基礎ファイルIEFには、前記したようにサーバ3でユーザ用に生成したm組の秘密鍵を内部認証鍵として記憶し、サーバ3用に生成したn組の秘密鍵を外部認証鍵として記憶する。

【0039】また、サーバ3のクライアント管理データベースにもユーザ用に生成した秘密鍵m組を外部認証鍵として記憶し、サーバ3用に生成した秘密鍵を内部認証鍵として記憶している。すなわち、内部認証鍵は、クライアント2がサーバ3を認証するための認証鍵であり、外部認証鍵は、サーバ3がクライアント2を認証するための認証鍵である。

【0040】内部認証鍵および外部認証鍵は、各々順番号の識別番号が付されている。以下では、ICカード5に記憶されているm番目の内部認証鍵を $k_{ai}[m]$ のように表示し、ICカード5に記憶されているn番目の外部認証鍵を $k_{ae}[n]$ のように表示する。また、サ

ーバ3で管理しているn番目の内部認証鍵を k_{si}

〔n〕と表示し、サーバ3で管理しているm番目の外部認証鍵を $k_{se}[m]$ と表示する。図3の例では、基礎ファイルIEF1、IEF2、IEF3、IEF4、IEF5、IEF6、IEF7の各々に、3つの内部認証鍵と4つの外部認証鍵、すなわち、 $k_{ai}[1]$ 、 $k_{ai}[2]$ 、 $k_{ai}[3]$ 、 $k_{ae}[1]$ 、 $k_{ae}[2]$ 、 $k_{ae}[3]$ 、 $k_{ae}[4]$ が格納されている。

【0041】ICカード5は、外部認証鍵、内部認証鍵を予め記憶した状態でネットワークシステム1のユーザに配布するものとする。ユーザは、このICカード5を所持し、ネットワークシステム1を利用するには、クライアント2のICカードリーダー6にICカード5を装填してクライアント2を操作する。

【0042】以上のようなシステム構成で、クライアント2からサーバ3に接続要求がされると、次のようにしてクライアント2とサーバ3との間の相互認証が行なわれる。図4は、この相互認証の手順を示す概念図である。なお、以下の説明で、 $E(K, R)$ は、RをKで暗号化することを示し、 $D(K, R)$ は、RをKで復号化することを示している。

【0043】相互認証にはICカード5に記憶されているm個の内部認証鍵、n個の外部認証鍵のうち一番番号の大きい、 $k_{ai}[m]$ 、 $k_{ae}[n]$ を用いる。まず、クライアント2から接続要求を受け取ったサーバ3は、乱数 R_s をクライアント2に送信する。クライアント2は、ICカード5に乱数 R_s を送信し、ICカード5のマイクロプロセッサ11では、 $E(K_{ai}[m], R_s)$ の処理、すなわち、不揮発性メモリ12に記憶されている識別番号がm番の内部認証鍵を用いて乱数 R_s を暗号化することで、内部認証コード C_{ai} に変換する。そして、この“内部認証コード $C_{ai}=E(K_{ai}[m], R_s)$ ”をクライアント2からサーバ3に送信する。

【0044】すると、サーバ3では、“ $D(K_{se}[m], C_{ai})$ ”の処理、すなわち、ICカード5用の外部認証鍵のうち識別番号がm番のものをクライアント管理データベースから呼出し、この外部認証鍵を用いて、“ $C_{ai}=E(K_{ai}[m], R_s)$ ”の復号化を行ない、そして、この復号化した C_{ai} と乱数 R_s とが一致するか否かを判断する。そして、一致するときは所定のOK信号を、一致しないときは所定のNG信号を、クライアント2に送信する。

【0045】このOK信号を受けたときは、クライアント2はICカード5に乱数を要求する。ICカード5は、この信号を受けて乱数 R_a をクライアント2に出力し、クライアント2は、この乱数 R_a をサーバ3に送信する。サーバ3では、 $E(K_{si}[n], R_a)$ の処理を行なう。すなわち、ICカード5用で識別番号がn番

の内部認証鍵を用いて乱数 R_a を暗号化することにより、サーバ3の内部認証コード、すなわち、クライアント2にとっての外部認証コード " $C_{si} = E(K_{si}[n], R_a)$ " に変換し、クライアント2に送信する。クライアント2は、この外部認証コード C_{si} をICカード5に送信し、ICカード5では、" $D(K_{ae}[n], C_{si})$ " の処理、すなわち、不揮発性メモリ12に記憶されている n 番の外部認証鍵で " $C_{si} = E(K_{si}[n], R_a)$ " を復号化し、復号化後の " $D(K_{ae}[n], C_{si})$ " が乱数 R_a に一致するか否かを判断する。一致するときは所定のOK信号を、一致しないときは所定のNG信号をクライアント2に送信し、クライアント2はサーバ3にOK信号、またはNG信号を送信する。

【0046】ICカード5が、サーバ3から配布された正当なICカードであるときは、サーバ3が管理している外部認証鍵 K_{se} と、ICカード5に記憶されている内部認証鍵 K_{ai} とは対応し、また、ICカード5に記憶されている外部認証鍵 K_{ae} と、サーバ3が管理している内部認証鍵 K_{si} とは対応するので、相互認証が成立する。

【0047】次に、この相互認証の成立後に行う暗号化データ通信の手順について説明する。図5は、認証鍵を利用してセッション鍵を生成する手順を示す概念図である。セッション鍵は、クライアント2/サーバ3間で共有して、クライアント2、サーバ3間の暗号化通信に使用するものである。

【0048】図5に示すように、前記相互認証が成立した後に、サーバ3は乱数 R_o をクライアント2に送信する。この乱数 R_o を受け取ったクライアント2は、ICカード5に内部認証を要求する。これを受けて、ICカード5は、 $E(K_{ai}[m], R_o)$ の処理を行なう。すなわち、不揮発性メモリ12に記憶されている識別番号が m 番の内部認証鍵を用いて乱数 R_o を暗号化し、この $E(K_{ai}[m], R_o)$ をセッション鍵として用い、サーバ3と暗号化通信を行なう。同様に、サーバ3も、 $E(K_{ai}[m], R_o)$ の処理、すなわち、クライアント管理データベースに記憶されている識別番号が m 番のクライアント2側の内部認証鍵を用いて乱数 R_o を暗号化し、この $E(K_{ai}[m], R_o)$ をセッション鍵として、対称鍵暗号方式によりクライアント2と暗号化通信を行なう。

【0049】つづいて、内部認証鍵、外部認証鍵の更新の手順について説明する。図6は、内部認証鍵、外部認証鍵を同時に更新するシーケンスの概念図である。一般にクライアント2/サーバ3間で相互認証、暗号化通信を行うには、前記のようにICカード5に記憶されている認証鍵のうち、一番番号の大きい $K_{ai}[m]$ 、 $K_{ae}[n]$ を使用する。図6に示すように、厩で新しい月になってクライアント2から最初の接続要求がサーバ3

にあったときに、図4を参照して前記した相互認証の処理に代えて、図6に示す処理を行う。

【0050】すなわち、サーバ3は、乱数 R_s のみならず、認証鍵の更新要求と、相互認証しようする認証鍵の識別番号をクライアント2に送信する。数字の一番大きな識別番号は、内部認証鍵については m 番、外部認証鍵については n 番であるので、相互認証しようする認証鍵の識別番号として、 m 番、 n 番の上位認証鍵、すなわち、 m 番、 n 番より1番ずつ少ない、外部認証鍵については $(m-1)$ 番、内部認証鍵については $(n-1)$ 番をクライアント2に送信する。

【0051】これを受け取ったクライアント2は、ICカード5に内部認証要求を行ない、ICカード5では、" $C_{ai} = E(K_{ai}[m-1], R_s)$ " を求め、この内部認証コード C_{ai} をクライアント2からサーバ3に送信する。そして、サーバ3では、" $R_s' = D(K_{se}[m-1], C_{ai})$ " を求め、そして、 R_s と R_s' とが一致するか否かを判断する。そして、一致するときはOK信号を、一致しないときはNG信号を、クライアント2に送信する。

【0052】クライアント2がOK信号を受けたときは、ICカード5に乱数を要求する信号を出力する。ICカード5は、この信号を受けて乱数 R_a をクライアント2に出力し、クライアント2は乱数 R_a をサーバ3に出力する。そして、サーバ3は、サーバ3の内部認証コード、すなわち、クライアント2にとっての外部認証コード " $C_{si} = E(K_{si}[n-1], R_a)$ " を生成し、クライアント2に送信し、クライアント2は、この外部認証コード C_{si} をICカード5に送信する。そして、ICカード5では、" $R_a' = D(K_{ae}[n-1], C_{si})$ " を求め、そして R_a と R_a' を比較して、一致するときはOK信号を、一致しないときはNG信号を、クライアント2に送り、上位認証鍵による相互認証が終了する。

【0053】この相互認証終了後に認証鍵更新の処理に入る。すなわち、サーバ3は乱数 R_{k1} 、 R_{k2} をクライアント2に送信する。また、サーバ3は、先程相互認証に用いたクライアント2側の内部認証鍵 $K_{ai}[m-1]$ を用いて、" $C_{s1} = E(K_{ai}[m-1], R_{k1})$ "、" $C_{s2} = E(K_{ai}[m-1], R_{k2})$ " を求める。

【0054】乱数 R_{k1} 、 R_{k2} を受けたクライアント2は、まず、乱数 R_{k1} を渡して、ICカード5に内部認証を要求する。すると、ICカード5は、" $C_{a1} = E(K_{ai}[m-1], R_{k1})$ " を求め、このコード C_{s1} をクライアント2に送ると、クライアント2はコード C_{a1} を新しい認証鍵とするようにICカード5に要求する。そして、ICカード5は、コード C_{a1} を m 番目の新しい内部認証鍵 $K_{ai}[m]$ として不揮発性メモリ12に記憶して、OK信号またはNG信号を

クライアント2に送る。

【0055】OK信号を受けたクライアント2は、次にRk2を渡して、ICカード5に内部認証を要求する。この要求を受けたICカード5は、“コードCa2=E(Kai[m-1], Rk2)”を求め、このコードCa2をクライアント2に送ると、クライアント2はコードCa2を新しい認証鍵とするようにICカード5に要求する。そして、ICカード5は、コードCa2をn番目の新しい内部認証鍵Kae[n]として不揮発性メモリ12に記憶し、OK信号またはNG信号をクライアント2に送る。クライアント2は受信したOK信号をサーバ3に送信する。OK信号を受けたサーバ3は、すでに求めてあるコードCs1を新しい外部認証鍵Kse[m]としてクライアント管理データベースに記憶し、また、すでに求めてあるコードCs2を新しい内部認証鍵Ksi[n]としてクライアント管理データベースに記憶して、認証鍵の更新を完了する。

【0056】このようにして、最も番号の大きい内部認証鍵、外部認証鍵の更新がなされるが、この更新を1か月に1度とはいえ、何度も繰り返していると、鍵の更新の際に使用している内部認証鍵Kai[m-1]、外部認証鍵Kae[n-1]も漏洩の可能性が高まる。そのような場合を考え、例えば1年に1度、内部認証鍵Kai[m-1]、外部認証鍵Kae[n-1]も更新する手続きをとるようにすればよい。その場合、更新の処理は図6を参照して説明した前記の処理と同様に行うことができる。すなわち、内部認証鍵Kai[m-2]、外部認証鍵Kae[n-2]を用いて、内部認証鍵Kai[m-1]、外部認証鍵Kae[n-1]を更新すればよい。以下、内部認証鍵Kai[m-2]、外部認証鍵Kae[n-2]、内部認証鍵Kai[m-3]、外部認証鍵Kae[n-3]、……についても同様である。

【0057】すなわち、かかる認証鍵の更新は、更新の際の内部認証鍵の総数をM、外部認証鍵の総数をNとしたときに、下式(1)で示されるm番目の内部認証鍵とn番目の外部認証鍵の更新を、識別番号が少なくともm番より小さい番号の内部認証鍵を用いてクライアント2がサーバ3を認証したことを条件に行なうもので、使用が稀である認証鍵により使用が頻繁な認証鍵m番目の内部認証鍵とn番目の外部認証鍵とを安全に更新するものである。

【0058】 $M-m=N-n \dots\dots(1)$

但し、上記の処理では、内部認証鍵Kai[1]、外部認証鍵Kae[1]は更新できないことになってしまう。内部認証鍵Kai[1]、外部認証鍵Kae[1]を更新する際には最初の相互認証そのものを内部認証鍵Kai[1]、外部認証鍵Kae[1]で行い、新しい鍵のもとになる乱数Rkから新しい内部認証鍵Kai[1]、外部認証鍵Kae[1]を生成する際も内部認証鍵Kai[1]を使用するという処理にしてもよい。

【0059】しかし、実際の運用を考えた場合、内部認証鍵Kai[1]、外部認証鍵Kae[1]を更新する要求が発生するのは、内部認証鍵Kai[1]、外部認証鍵Kae[1]が漏洩した可能性がある場合である。その場合に、内部認証鍵Kai[1]、外部認証鍵Kae[1]を用いて鍵の更新を行うのは意味をなさない可能性があるため、内部認証鍵Kai[1]、外部認証鍵Kae[1]を更新する必要がある場合は、ICカード5を鍵発行センタであるサーバ3に持参するか、ICカード5を破棄して新しいICカード5をサーバ3から受け取るのが望ましい。

【0060】前記の例では、対称鍵暗号系を用いる場合について説明した。非対称鍵暗号系を用いる場合は次のようにする。

【0061】すなわち、サーバ3は、各ユーザに対応して、ユーザ用に秘密鍵と公開鍵のペアをm組生成し、また、サーバ3用に秘密鍵と公開鍵のペアをn組生成する。そして、サーバ3のクライアント管理データベースには、サーバ3が生成したすべての秘密鍵、公開鍵を記憶する。

【0062】基礎ファイルIEFには、サーバ3でユーザ用にm組の秘密鍵と公開鍵のペアを生成して、そのうちの秘密鍵を内部認証鍵として記憶し、サーバ3用にn組の秘密鍵と公開鍵のペアを生成して、そのうちの公開鍵を外部認証鍵として記憶する。

【0063】また、サーバ3のクライアント管理データベースは、サーバ3でユーザ用に生成した秘密鍵と公開鍵のペアのうちm組ある公開鍵を外部認証鍵として記憶し、サーバ3用に生成した秘密鍵と公開鍵のペアのうちn組ある秘密鍵を内部認証鍵として記憶する。

【0064】以上の各点については、以下の各実施の形態で非対称鍵暗号系を用いる場合の説明においても同様である。

【0065】以上のようにすることで、非対称鍵暗号系を用いる場合においても、その相互認証、セッション鍵の交換により行う暗号化データ通信、認証鍵の更新の処理は、図4～図6を参照して説明した対称鍵暗号系の場合と同様に行うことができる。なお、非対称鍵暗号系を用いて相互認証やセッション鍵交換を行う場合でも、暗号化データ通信を行う場合は対称鍵暗号方式を用いるのが一般的である。

【0066】【発明の第2の実施の形態】この実施の形態は、相互認証、セッション鍵を交換して行う暗号化データ通信の手順は前記第1の実施の形態と同様であり、図示、説明は省略する。前記第1の実施の形態と同様の部材等については以下の説明で同一符号を付して説明する。

【0067】この実施の形態では、認証鍵の更新のシーケンスが前記第1の実施の形態の場合と異なる。すなわち、前記第1の実施の形態では、外部認証鍵と内部認証

鍵とを一度に更新しているが、この実施の形態は個別的に更新を行うものである。

【0068】図7は、この実施の形態の外部認証鍵の更新のシーケンスを示すブロック図である。但し、前記第1の実施の形態における図6に示すような上位認証鍵による相互認証の手続きは図示を省略しており、以下の説明でも省略する。すなわち、上位認証鍵による相互認証の手続きが完了すると、サーバ3からクライアント2に乱数 $Rk2$ を送信する。また、サーバ3は“コード $Cs2 = E(Kai[m-1], Rk2)$ ”を求める。クライアント2はICカード5に乱数 $Rk2$ を送信し、内部認証を要求する。するとICカード5は、“コード $Ca2 = E(Kai[m-1], Rk2)$ ”を求め、このコード $Ca2$ をクライアント2に送信する。すると、クライアント2はコード $Ca2$ を新しい認証鍵とするようにICカード5に要求する。そして、ICカード5は、コード $Ca2$ を n 番目の新しい内部認証鍵 $Kae[n]$ として不揮発性メモリ12に記憶し、OK信号またはNG信号をクライアント2に送る。クライアント2は受信したOK信号をサーバ3に送信する。OK信号を受けたサーバ3は、すでに求めてあるコード $Cs2$ を新しい外部認証鍵 $Ksi[m]$ としてクライアント管理データベースに記憶して、最も番号の大きい内部認証鍵 $Kai[m]$ の更新を完了する。

【0069】図8は、この実施の形態の内部認証鍵の更新のシーケンスを示すブロック図である。但し、前記第1の実施の形態における図6に示すような上位認証鍵による相互認証の手続きは図示を省略しており、以下の説明でも省略する。すなわち、上位認証鍵による相互認証の手続きが完了すると、サーバ3からクライアント2に乱数 $Rk1$ を送信する。また、サーバ3は“コード $Cs1 = E(Kai[m-1], Rk1)$ ”を求める。クライアント2はICカード5に乱数 $Rk1$ を送信し、内部認証を要求する。するとICカード5は、“コード $Ca1 = E(Kai[m-1], Rk1)$ ”を求め、このコード $Ca1$ をクライアント2に送信する。すると、クライアント2はコード $Ca1$ を新しい認証鍵とするようにICカード5に要求する。そして、ICカード5は、コード $Ca1$ を n 番目の新しい内部認証鍵 $Kai[n]$ として不揮発性メモリ12に記憶し、OK信号またはNG信号をクライアント2に送る。クライアント2は受信したOK信号をサーバ3に送信する。OK信号を受けたサーバ3は、すでに求めてあるコード $Cs1$ を新しい内部認証鍵 $Kse[m]$ としてクライアント管理データベースに記憶して、最も番号の大きい外部認証鍵 $Kae[n]$ の更新を完了する。

【0070】〔発明の第3の実施の形態〕この実施の形態も、相互認証、セッション鍵を用いて行う暗号化データ通信の手順は前記第1の実施の形態と同様であり、図示、説明は省略する。前記第1の実施の形態と同様の部

材等については以下の説明で同一符号を付して説明する。

【0071】この実施の形態も、認証鍵の更新のシーケンスが前記第1の実施の形態の場合と異なる。すなわち、前記第1の実施の形態では、最も番号の大きい外部認証鍵と内部認証鍵のみを一度に更新しているが、この実施の形態は複数の外部認証鍵と内部認証鍵を一度に更新するものである。

【0072】図9は、この実施の形態の外部認証鍵、内部認証鍵の更新のシーケンスを示すブロック図である。但し、前記第1の実施の形態における図6に示すような上位認証鍵による相互認証の手続きは図示を省略しており、以下の説明でも省略する。すなわち、上位認証鍵による相互認証の手続きが完了すると、前記第1の実施の形態と同様、認証鍵更新の処理に入る。

【0073】すなわち、サーバ3は乱数 $Rk1, Rk2, Rk3, Rk4, ……$ をクライアント2に送信する。また、サーバ3は、先程相互認証に用いた内部認証鍵 $Kai[m-1]$ を用いて、“コード $Cs1 = E(Kai[m-1], Rk1)$ ”、“コード $Cs2 = E(Kai[m-1], Rk2)$ ”、“コード $Cs3 = E(Kai[m-1], Rk3)$ ”、“コード $Cs4 = E(Kai[m-1], Rk4)$ ”、……を求める。

【0074】乱数 $Rk1, Rk2, Rk3, Rk4, ……$ を受けたクライアント2は、乱数 $Rk1, Rk2, Rk3, Rk4, ……$ を送信し、ICカード5に内部認証を要求する。すると、ICカード5は、“コード $Ca1 = E(Kai[m-1], Rk1)$ ”を求め、このコード $Ca1$ をクライアント2に送ると、クライアント2はコード $Ca1$ を新しい認証鍵とするようにICカード5に要求する。そして、ICカード5は、コード $Ca1$ を m 番目の新しい内部認証鍵 $Kai[m]$ として不揮発性メモリ12に記憶して、OK信号またはNG信号をクライアント2に送る。

【0075】OK信号を受けたクライアント2は、ICカード5に内部認証を要求する。この要求を受けたICカード5は、“コード $Ca2 = E(Kai[m-1], Rk2)$ ”を求め、このコード $Ca2$ をクライアント2に送ると、クライアント2はコード $Ca2$ を新しい認証鍵とするようにICカード5に要求する。そして、ICカード5は、コード $Ca2$ を n 番目の新しい外部認証鍵 $Kae[n]$ として不揮発性メモリ12に記憶し、OK信号またはNG信号をクライアント2に送る。

【0076】OK信号を受けたクライアント2は、ICカード5に内部認証を要求する。すると、ICカード5は、“コード $Ca3 = E(Kai[m-1], Rk3)$ ”を求め、このコード $Ca3$ をクライアント2に送ると、クライアント2はコード $Ca3$ を新しい認証鍵とするようにICカード5に要求する。そして、ICカード5は、コード $Ca3$ を $m+1$ 番目の新しい内部認証鍵

$K_{ai}[m+1]$ として不揮発性メモリ12に記憶して、OK信号またはNG信号をクライアント2に送る。

【0077】OK信号を受けたクライアント2は、ICカード5に内部認証を要求する。この要求を受けたICカード5は、“コード $C_{a4}=E(K_{ai}[m-1], R_{k4})$ ”を求め、このコード C_{a4} をクライアント2に送ると、クライアント2はコード C_{a4} を新しい認証鍵とするようにICカード5に要求する。そして、ICカード5は、コード C_{a4} をn番目の新しい外部認証鍵 $K_{ae}[n+1]$ として不揮発性メモリ12に記憶し、OK信号またはNG信号をクライアント2に送る。

【0078】以上のような処理を繰り返した後、クライアント2は受信したOK信号をサーバ3に送信する。OK信号を受けたサーバ3は、すでに求めてあるコード C_{a1} を新しい外部認証鍵 $K_{se}[m]$ とし、また、コード C_{a2} を新しい内部認証鍵 $K_{si}[n]$ とし、コード C_{s3} を新しい外部認証鍵 $K_{se}[m+1]$ とし、また、コード C_{s4} を新しい内部認証鍵 $K_{si}[n+1]$ 、……として、クライアント管理データベースに記憶し、認証鍵の更新を完了する。

【0079】〔発明の第4の実施の形態〕この実施の形態も、相互認証、セッション鍵を用いて行う暗号化データ通信の手順は前記第1の実施の形態と同様であり、図示、説明は省略する。前記第1の実施の形態と同様の部材等については以下の説明で同一符号を付して説明する。

【0080】この実施の形態も、認証鍵の更新のシーケンスが前記第1の実施の形態の場合と異なる。すなわち、前記第1の実施の形態では、ICカード5で新たな認証鍵を計算し、その結果をクライアント2に送信しているが、この実施の形態では、クライアント2に送信せずに、新たな認証鍵の計算し、それをICカード5内に設定するものである。

【0081】図10は、この実施の形態の外部認証鍵、内部認証鍵の更新のシーケンスを示すブロック図である。但し、前記第1の実施の形態における図6に示すような上位認証鍵による相互認証の手続きは図示を省略しており、以下の説明でも省略する。すなわち、上位認証鍵による相互認証の手続きが完了すると、前記第1の実施の形態と同様、認証鍵更新の処理に入る。

【0082】すなわち、サーバ3は乱数 R_{k1} 、 R_{k2} をクライアント2に送信する。また、サーバ3は、先程相互認証に用いた内部認証鍵 $K_{ai}[m-1]$ を用いて、“コード $C_{s1}=E(K_{ai}[m-1], R_{k1})$ ”、“コード $C_{s2}=E(K_{ai}[m-1], R_{k2})$ ”を求める。

【0083】乱数 R_{k1} 、 R_{k2} を受けたクライアント2は、乱数 R_{k1} 、 R_{k2} を送信し、ICカード5に内部認証を要求する。すると、ICカード5は、“コード $C_{a1}=E(K_{ai}[m-1], R_{k1})$ ”を求め、こ

のコード C_{a1} をクライアント2に送ることなく、コード C_{a1} をm番目の新しい内部認証鍵 $K_{ai}[m]$ として不揮発性メモリ12に記憶して、OK信号またはNG信号をクライアント2に送る。

【0084】OK信号を受けたクライアント2はICカード5に内部認証を要求する。この要求を受けたICカード5は、“コード $C_{a2}=E(K_{ai}[m-1], R_{k2})$ ”を求め、このコード C_{a2} をクライアント2に送ることなく、コード C_{a2} をn番目の新しい内部認証鍵 $K_{ae}[n]$ として不揮発性メモリ12に記憶し、OK信号またはNG信号をクライアント2に送る。クライアント2は受信したOK信号をサーバ3に送信する。OK信号を受けたサーバ3は、すでに求めてあるコード C_{a1} を新しい外部認証鍵 $K_{se}[m]$ としてクライアント管理データベースに記憶し、また、すでに求めてあるコード C_{s2} を新しい内部認証鍵 $K_{si}[n]$ としてクライアント管理データベースに記憶して、1番大きな番号の認証鍵の更新を完了する。

【0085】内部認証鍵 $K_{ai}[m-1]$ 、外部認証鍵 $K_{ae}[n-1]$ 、内部認証鍵 $K_{ai}[m-2]$ 、外部認証鍵 $K_{ae}[n-2]$ 、……の更新についても、前記と同様に更新することができる。

【0086】なお、いうまでもなく、前記各実施の形態は、この発明を限定するものではない。

【0087】例えば、前記各実施例で、サーバ3では、“ $D(K_{se}[m], E(K_{ai}[m], R_s))$ ”の処理を行い、そして、この復号化した“ $D(K_{se}[m], E(K_{ai}[m], R_s))$ ”と乱数 R_s とが一致するか否かを判断しているが、対称鍵暗号系を用いる場合は、これに代えて、 $E(K_{se}[m], R_s)$ と $E(K_{ai}[m], R_s)$ とが一致するか否かを判断するようにしてもよいし、前記の例では、ICカード5で“ $D(K_{ae}[n], E(K_{si}[n], R_a))$ ”の処理を行い、そして、この復号化した“ $D(K_{ae}[n], E(K_{si}[n], R_a))$ ”と乱数 R_a とが一致するか否かを判断しているが、これに代えて、 $E(K_{ae}[n], R_a)$ と $E(K_{si}[n], R_a)$ とが一致するか否かを判断するようにしてもよい。

【0088】また、前記第1、第2、第4の実施の形態で、乱数 R_{k1} 、 R_{k2} の両方を送信しなくても、乱数 R_{k1} のみを送信し、この R_{k1} の補数を乱数 R_{k2} の代わりに用いるというように、 R_{k1} から R_{k2} を導き出すようにしてもよい。

【0089】

〔発明の効果〕請求項1に記載の発明は、通信回線を介して接続されているクライアントとサーバとの間の相互認証に使用する認証鍵を格納している記憶媒体をユーザが所持し、この記憶媒体と前記クライアントを接続して、前記認証鍵を用いた前記相互認証を行なった後、前記認証鍵に基づいてセッション鍵を生成して暗号化通信

を行なうネットワークシステムであって、前記認証鍵は前記記憶媒体に複数個記憶して、定期または不定期に更新して用い、この更新を前記複数の認証鍵のうちいずれかのものに対して行なうには、少なくとも当該認証鍵以外の前記認証鍵を用いて行なう前記相互認証が成立した後に、前記サーバから乱数を前記クライアントに送信し、前記相互認証に用いた前記認証鍵を用いて前記乱数から更新にかかる前記認証鍵を新たに生成して前記記憶媒体に記憶することにより行なうものであることを特徴とするものであるため、相互認証が成立した後に、サーバから乱数をクライアントに送信し、相互認証に用いた認証鍵を用いて乱数から更新にかかる認証鍵を新たに暗号化や復号化などで生成することができるので、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、認証鍵を更新することができる。

【0090】請求項2に記載の発明は、請求項1に記載の発明において、記憶媒体は、クライアントがサーバを認証するための認証鍵である外部認証鍵と、前記サーバが前記クライアントを認証するための認証鍵である内部認証鍵とをいずれも識別番号を付して複数個ずつ記憶していて、前記内部認証鍵および前記外部認証鍵を用いて相互認証を行なうものであることを特徴とするものであるため、相互認証が成立した後に、サーバから乱数をクライアントに送信し、相互認証に用いた内部認証鍵を用いて乱数から更新にかかる内部認証鍵、外部認証鍵を新たに生成することができるので、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、内部認証鍵、外部認証鍵を更新することができる。

【0091】請求項3に記載の発明は、請求項2に記載の発明において、複数の内部認証鍵のうち識別番号がm番のものを更新するには、外部認証鍵と少なくともこのm番の内部認証鍵以外の内部認証鍵とを用いて行なう相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記m番の内部認証鍵を新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とするものであるため、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、識別番号がm番の内部認証鍵を更新することができる。

【0092】請求項4に記載の発明は、請求項2または3のいずれかに記載の発明において、複数の外部認証鍵のうち識別番号がn番のものを更新するには、内部認証鍵と少なくともこのn番の外部認証鍵以外の外部認証鍵とを用いて行なう相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記n番の外部認証鍵を新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とするものであるため、通信アルゴリズムが対称鍵暗号方式か、非対称

鍵暗号方式かに依存せずに識別番号がn番の外部認証鍵を更新することができる。

【0093】請求項5に記載の発明は、請求項2、3、4のいずれかに記載の発明において、複数の内部認証鍵のうち識別番号がm番のものおよび複数の外部認証鍵のうち識別番号がn番目のものを一度に更新するには、少なくとも前記m番の内部認証鍵以外の内部認証鍵と少なくとも前記n番の外部認証鍵以外の外部認証鍵とを用いて行なう相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記m番の内部認証鍵と前記n番の外部認証鍵とを新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とするものであるため、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、少ない鍵更新処理により安全に、識別番号がm番の内部認証鍵と識別番号がn番の外部認証鍵を一度に更新することができる。

【0094】請求項6に記載の発明は、請求項2、3、4、5のいずれかに記載の発明において、複数の内部認証鍵を一度に更新するには、外部認証鍵と識別番号がm番より小さい内部認証鍵とを用いて相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記識別番号がm番以上の各内部認証鍵を新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とするものであるため、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、少ない鍵更新処理により安全に、複数の内部認証鍵を一度に更新することができる。

【0095】請求項7に記載の発明は、請求項2、3、4、5、6のいずれかに記載の発明において、複数の外部認証鍵を一度に更新するには、内部認証鍵と識別番号がn番より小さい外部認証鍵とを用いて相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から前記識別番号がn番以上の各外部認証鍵を新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とするものであるため、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、少ない鍵更新処理により安全に、複数の外部認証鍵を一度に更新することができる。

【0096】請求項8に記載の発明は、請求項2、3、4、5、6、7のいずれかに記載の発明において、複数の内部認証鍵と複数の外部認証鍵とを一度に更新するには、識別番号がm番より小さい内部認証鍵と識別番号がn番より小さい外部認証鍵とを用いて行なう相互認証が成立した後に、サーバから乱数をクライアントに送信し、前記クライアントは前記相互認証に用いた内部認証鍵を用いて前記乱数から識別番号がm番以上の内部認証

鍵と識別番号が n 番移動の外部認証鍵とを新たに生成して記憶媒体に記憶することにより行なうものであることを特徴とするものであるため、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、少ない鍵更新処理により安全に、複数の内部認証鍵と複数の外部認証鍵とを一度に更新することができる。

【0097】請求項 9 に記載の発明は、請求項 2、3、4、5、6、7、8 のいずれかに記載の発明において、更新の際の内部認証鍵の総数を M 、外部認証鍵の総数を N としたときに、下式で示される m 番目の内部認証鍵と n 番目の外部認証鍵の更新は、識別番号が少なくとも n 番より小さい番号の外部認証鍵を用いてクライアントがサーバを認証したことを条件に行なうものであることを特徴とするものであるため、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、使用が稀である認証鍵により使用が頻繁な認証鍵 m 番目の内部認証鍵と n 番目の外部認証鍵とを安全に更新することができる。

【0098】 $M - m = N - n$

請求項 10 に記載の発明は、請求項 2、3、4、5、6、7、8、9 のいずれかに記載の発明において、記憶媒体は、更新に先立って行なわれた相互認証に使用した認証鍵を用いサーバがクライアントに送信した乱数から新たな認証鍵の生成を行なって、この生成後の新たな認証鍵を記憶媒体内部の不揮発性メモリにのみ記憶するものであることを特徴とするものであるため、通信アルゴリズムが対称鍵暗号方式か、非対称鍵暗号方式かに依存せずに、更新後の新たな認証鍵を記憶媒体外に漏らすことなく認証鍵を安全に更新することができる。

【0099】請求項 11 に記載の発明は、請求項 2、3、4、5、6、7、8、9、10 のいずれかに記載の発明において、記憶媒体として IC カードを用いることを特徴とするものであるため、一般に普及し始めている IC カードを記憶媒体としてもちい、ネットワークシ

テムを低コストで構築することができる。

【図面の簡単な説明】

【図 1】この発明の第 1 の実施の形態にかかるネットワークシステムの概略構成を示すブロック図である。

【図 2】前記ネットワークシステムに用いる IC カードの回路構成を示すブロック図である。

【図 3】前記 IC カード内の不揮発メモリ内の認証鍵のファイルフォーマットの一例を示すブロック図である。

【図 4】前記ネットワークシステムにおける相互認証の処理手順を示すブロック図である。

【図 5】前記ネットワークシステムにおける暗号化データ通信に用いるセッション鍵の生成の手順を示すブロック図である。

【図 6】前記ネットワークシステムにおける内部認証鍵、外部認証鍵の更新の手順を示すブロック図である。

【図 7】この発明の第 2 の実施の形態にかかるネットワークシステムにおける外部認証鍵の更新手順を示すブロック図である。

【図 8】この発明の第 2 の実施の形態にかかるネットワークシステムにおける内部認証鍵の更新手順を示すブロック図である。

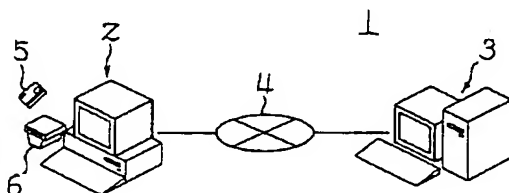
【図 9】この発明の第 3 の実施の形態にかかるネットワークシステムにおける内部認証鍵、外部認証鍵の更新手順を示すブロック図である。

【図 10】この発明の第 4 の実施の形態にかかるネットワークシステムにおける内部認証鍵、外部認証鍵の更新手順を示すブロック図である。

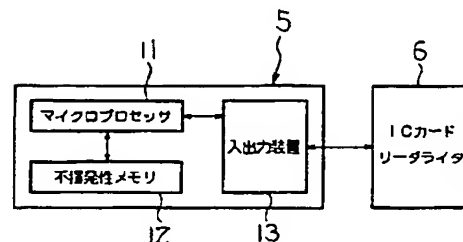
【符号の説明】

- 1 ネットワークシステム
- 2 クライアント
- 3 サーバ
- 4 通信回線
- 5 記憶媒体 (IC カード)
- 12 不揮発性メモリ

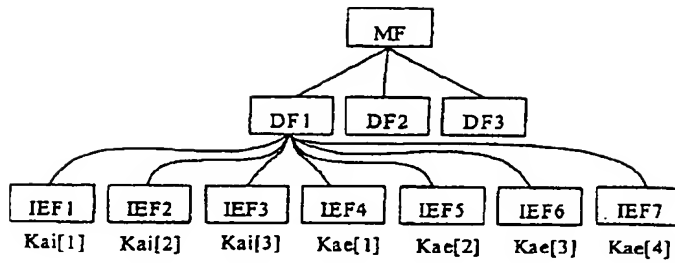
【図 1】



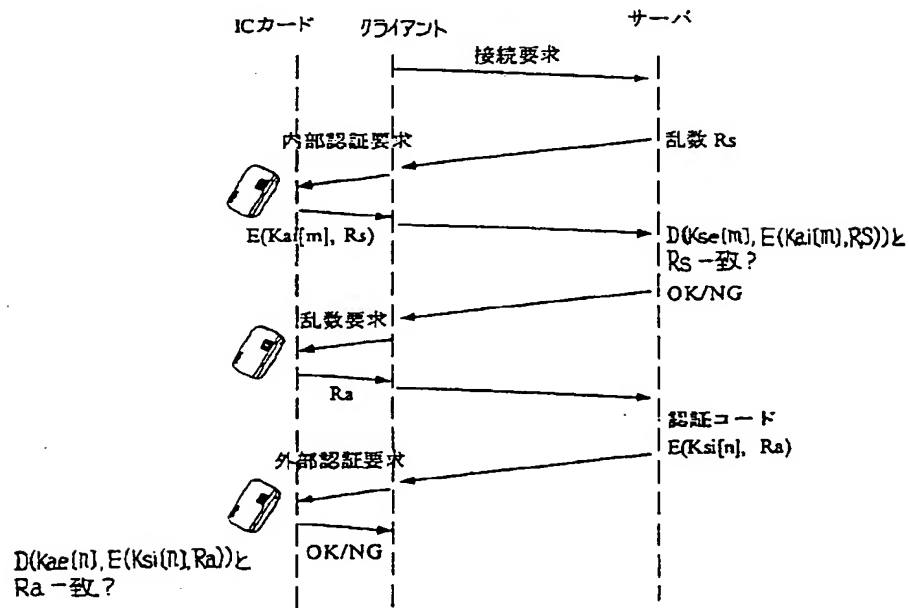
【図 2】



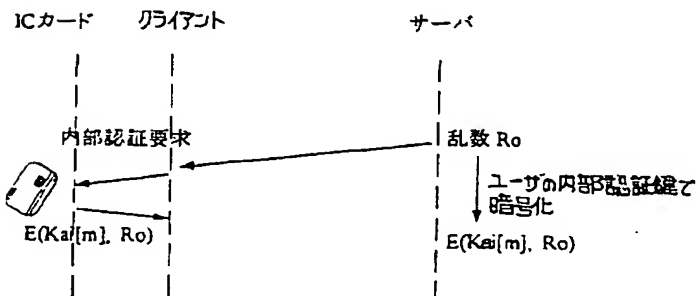
【図 3】



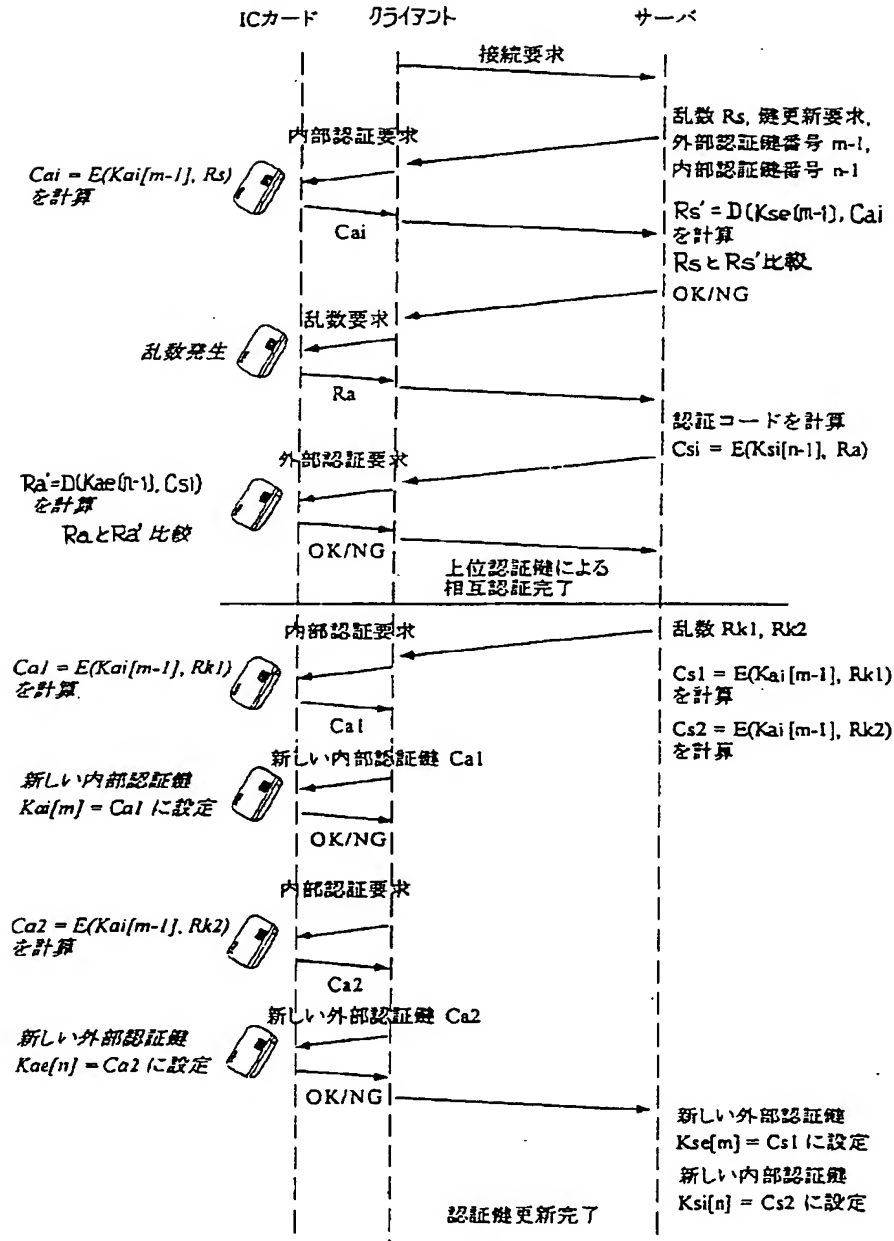
【図 4】



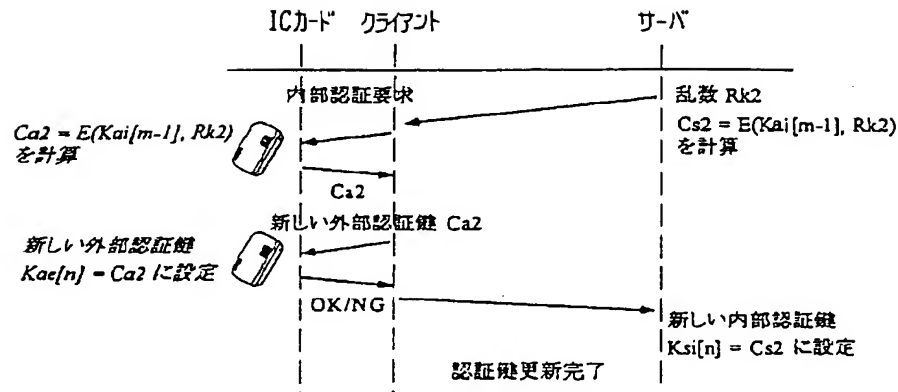
【図 5】



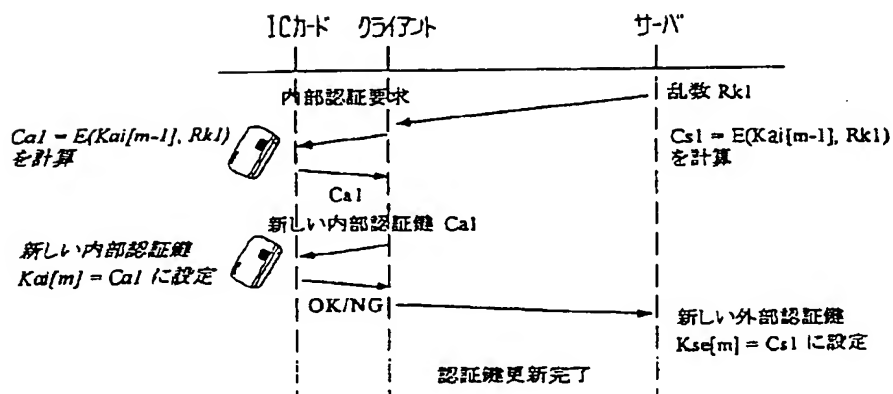
【図6】



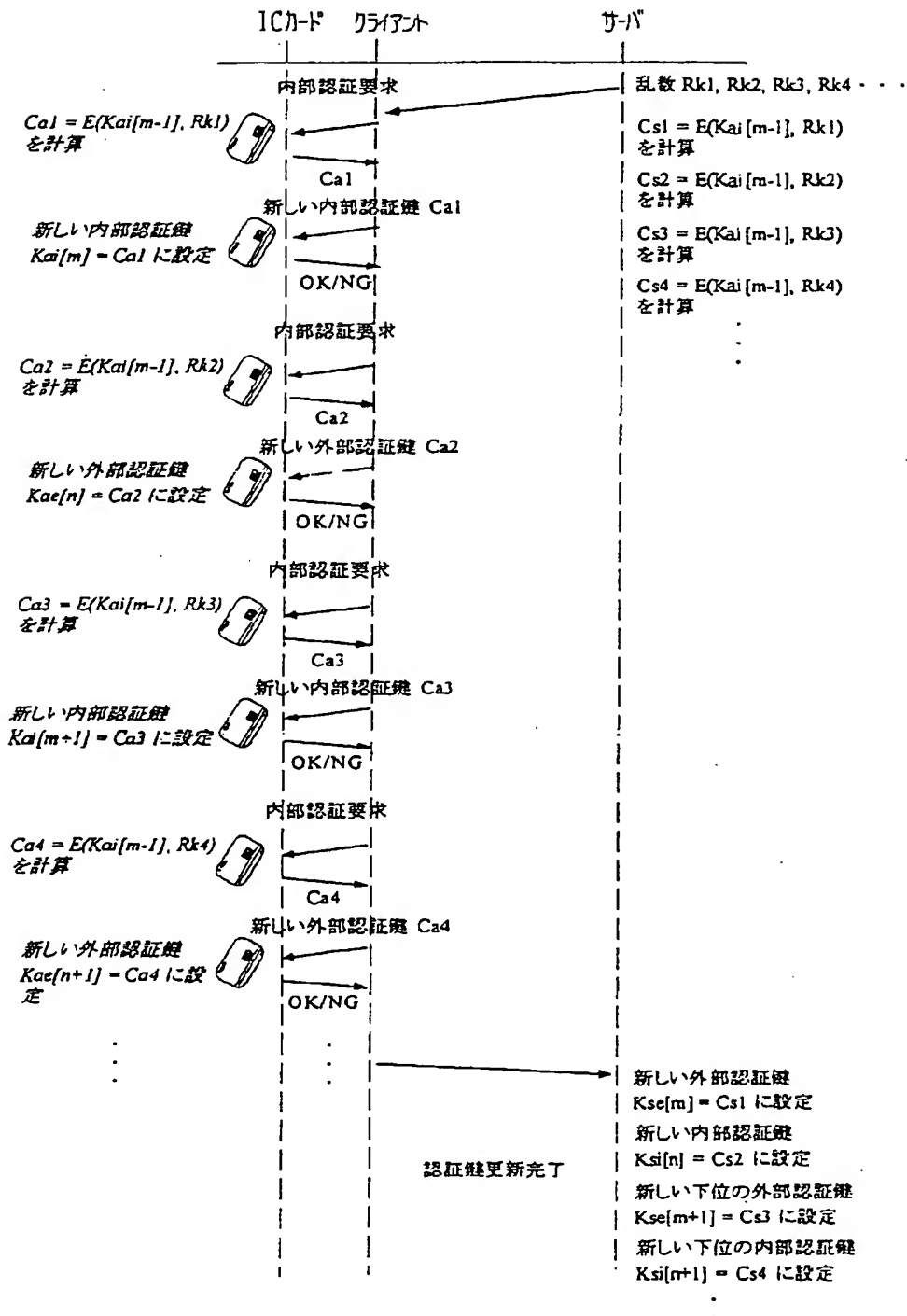
【図 7】



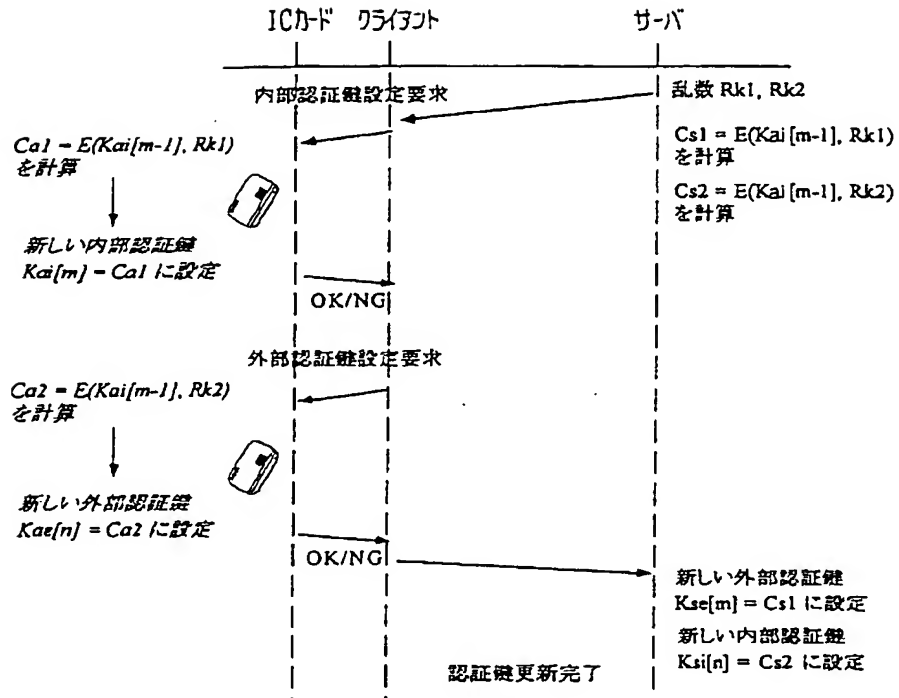
【図 8】



【図 9】



【図 10】



フロントページの続き

(51) Int. Cl. 6

識別記号

F I

H O 4 L 9/00

6 7 5 A